ABELIAN VARIETIES WITHOUT HOMOTHETIES

YURI G. ZARHIN

ABSTRACT. A celebrated theorem of Bogomolov asserts that the ℓ-adic Lie algebra attached to the Galois action on the Tate module of an abelian variety over a number field contains all homotheties. This is not the case in characteristic p: a "counterexample" is provided by an ordinary elliptic curve defined over a finite field. In this note we discuss (and explicitly construct) more interesting examples of "non-constant" absolutely simple abelian varieties (without homotheties) over global fields in characteristic p.

1. INTRODUCTION

Let K be a field, K_a its algebraic closure and $\mathrm{Gal}(K) = \mathrm{Aut}(K_a/K)$ the absolute Galois group. If X is an abelian variety over K then we write $\mathrm{End}_K(X)$ for the ring of K-endomorphisms of X and $\mathrm{End}_K^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}_K(X) \otimes \mathbb{Q}$. We write $\mathrm{End}(X)$ for the ring of K_a-endomorphisms of X and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$. The notation 1_X stands for the identity automorphism of X. It is well-known [5] that $\mathrm{End}^0(X)$ is a finite-dimensional semisimple $\mathbb{Q}$-algebra and its center $\mathfrak{C}(X)$ is a product of number fields; in addition, either of those fields is either totally real or a CM-field.

Let E be a number field. Suppose we are given an embedding

$$i : E \hookrightarrow \mathrm{End}_K^0(X),\ i(1) = 1_X.$$

Then $[E : \mathbb{Q}]$ divides $2\mathrm{dim}(X)$ [15, Ch. 2, Sect. 5, Prop. 2]; let us put

$$r(X, E) = \frac{2\mathrm{dim}(X)}{[E : \mathbb{Q}]}.$$

Let ℓ be a prime different from $\mathrm{char}(K)$. We write $T_\ell(X)$ for the corresponding Tate $\mathbb{Z}_\ell$-module of X and $V_\ell(X)$ for the corresponding $\mathbb{Q}_\ell$-vector space $T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. It is well-known that $T_\ell(X)$ is a free $\mathbb{Z}_\ell$-module of rank $2\mathrm{dim}(X)$ and $V_\ell(X)$ is a $2\mathrm{dim}(X)$-dimensional $\mathbb{Q}_\ell$-vector space. We write Id for the identity automorphism of $V_\ell(X)$. It is well-known that $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \cong \mathrm{GL}(2\mathrm{dim}(X), \mathbb{Z}_\ell)$ is a compact ℓ-adic Lie group with Lie algebra $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$. Let

$$\det : \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X)) \to \mathbb{Q}_\ell^*$$

be the determinant map. As usual, we write $\mathrm{SL}(V_\ell(X))$ for its kernel. It is well-known that $\mathrm{SL}(V_\ell(X))$ is a Lie subgroup in $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$ and its Lie algebra coincides with

$$\mathfrak{sl}(V_\ell(X)) := \{u \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)) \mid \mathrm{tr}(u) = 0\}$$

where

$$\mathrm{tr} : \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)) \to \mathbb{Q}_\ell$$

is the trace map.

On the other hand, $T_\ell(X)$ carries a natural structure of $\mathrm{End}_K(X)\otimes\mathbb{Z}_\ell$-module and $V_\ell(X)$ carries a natural structure of $\mathrm{End}^0_K(X)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module.

Let us put

$$E_\ell = E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell \subset \mathrm{End}^0_K(X)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell.$$

The embedding i provides $V_\ell(X)$ with a natural structure of E_ℓ-module: it is known [14, 9] that this module is free of rank $r(X,E)$.

One may view E_ℓ^* as a commutative ℓ-adic Lie (sub)group with (commutative) Lie algebra E_ℓ. We have

$$\mathbb{Z}_\ell^*\mathrm{Id}\subset E_\ell^*\subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X));$$

clearly, $\mathbb{Z}_\ell^*\mathrm{Id}$ is a compact ℓ-adic Lie subgroup whose Lie algebra coincides with $\mathbb{Q}_\ell\mathrm{Id}$.

Remark 1.1. Let $G\subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$ be a compact subgroup. Then the (ℓ-adic variant of) Cartan's theorem [13, Part 2, Ch. 5, Sect. 9] tells us that G is a Lie subgroup. Clearly, the intersection $G\bigcap\mathbb{Z}_\ell^*\mathrm{Id}$ is infinite if and only if the Lie algebra $\mathrm{Lie}(G)$ of G contains $\mathbb{Q}_\ell\mathrm{Id}$.

Let us consider the centralizer $\mathrm{End}_{E_\ell}(V_\ell(X))$ of E_ℓ in $\mathrm{End}_{Q_\ell}(V_\ell(X))$ and its group of invertible elements $\mathrm{Aut}_{E_\ell}(V_\ell(X))$. One may view $\mathrm{Aut}_{E_\ell}(V_\ell(X))$ as an ℓ-adic Lie group with Lie algebra $\mathrm{End}_{E_\ell}(V_\ell(X))$.

Since $V_\ell(X)$ is a free E_ℓ-module of finite rank, there are the natural E_ℓ-determinant homomorphism of ℓ-adic Lie groups

$$\det{}_{E_\ell}:\mathrm{Aut}_{E_\ell}(V_\ell(X))\to E_\ell^*$$

and the E_ℓ-trace map

$$\mathrm{tr}_{E_\ell}:\mathrm{End}_{E_\ell}(V_\ell(X))\to E_\ell.$$

Clearly, tr_{E_ℓ} is the *tangent map* of Lie algebras attached to $\det{}_{E_\ell}$.

Remark 1.2. Let G be a (closed) compact subgroup in $\mathrm{Aut}_{E_\ell}(V_\ell(X))$. Then G is an ℓ-adic Lie (sub)group and its Lie algebra $\mathrm{Lie}(G)$ is a $\mathbb{Q}_\ell$-Lie subalgebra of $\mathrm{End}_{E_\ell}(V_\ell(X))$. In addition, if $\mathrm{Lie}(G)$ is a semisimple Lie algebra then $\det{}_{E_\ell}(G)$ is a finite subgroup in E_ℓ^*. Indeed, the semisimplicity of $\mathrm{Lie}(G)$ implies that $\mathrm{tr}_{E_\ell}(\mathrm{Lie}(G))=\{0\}$ and therefore $\det{}_{E_\ell}=1$ on an open subgroup of G. One has only to recall that every open subgroup in a compact ℓ-adic Lie group has finite index.

There is a natural continuous homomorphism (ℓ-adic representation) [10]

$$\rho_{\ell,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X))\subset\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X));$$

its image $G_{\ell,X}$ is a compact ℓ-adic Lie subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$. We write $\mathfrak{g}_{\ell,X}$ for the Lie algebra of $G_{\ell,X}$; one may view $\mathfrak{g}_{\ell,X}$ as a Lie $\mathbb{Q}_\ell$-subalgebra in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$ [10].

The following assertion is proven in [18].

Theorem 1.3. *Suppose that K is a global field of characteristic $p>2$ and X is an abelian variety of positive dimension over K. Then:*

(I) $\mathfrak{g}_{\ell,X}$ *is a reductive $\mathbb{Q}_\ell$ algebra, i.e. $\mathfrak{g}_{\ell,X}\cong\mathfrak{g}^{ss}\oplus\mathfrak{c}$ where $\mathfrak{g}^{ss}$ is a semisimple $\mathbb{Q}_\ell$-Lie algera and $\mathfrak{c}$ is the center of $\mathfrak{g}_{\ell,X}$.*

(II) $\dim_{\mathbb{Q}_\ell}(\mathfrak{c})=1$.

(III) *If $\mathfrak{C}(X)$ is a product of totally real number fields then $\mathfrak{c}=\mathbb{Q}_\ell\cdot\mathrm{Id}$.*

When K is a number field, a theorem of Bogomolov [1, 2] asserts that $\mathfrak{g}_{\ell,X}$ always contains homotheties $\mathbb{Q}_\ell \cdot \mathrm{Id}$.

However, one may easily check that this is not the case if K is a global field of characteristic p. For example, if X is an ordinary elliptic curve that is defined over a finite field then $\mathfrak{g}_{\ell,X}$ is a one-dimensional $\mathbb{Q}_\ell$-Lie algebra that is generated by the ℓ-adic logarithm of the corresponding Frobenius endomorphism, which is not a scalar. The aim of this note is to prove the existence of an absolutely simple abelian variety X over a global field of characteristic p such that $\mathfrak{g}_{\ell,X}$ does *not* contain homotheties and X is *not* isogenous over K_a to an abelian variety over a finite field. Recall [6] that the latter condition means that X is not an abelian variety of CM-type over K_a. Our main result is described by the following two statements.

Theorem 1.4. *Suppose that K is a global field of characteristic $p > 2$. Suppose that X is an ordinary abelian variety of positive dimension over K. Let $E \subset \mathrm{End}^0(X)$ be a subfield that contains 1_X. Assume that $r(X,E)$ is an odd integer.*

Then $\mathfrak{g}_{\ell,X} \bigcap \mathbb{Q}_\ell \cdot \mathrm{Id} = \{0\}$, i.e., $\mathfrak{g}_{\ell,X}$ does not contain homotheties except zero and $G_{\ell,X} \bigcap \mathbb{Z}_\ell^* \mathrm{Id}$ is finite.

We prove Theorem 1.4 in Section 3.

Theorem 1.5. *Let Z be an ordinary elliptic curve over a finite field k of characteristic $p > 2$ and $E = \mathrm{End}^0(Z)$ the corresponding imaginary quadratic field.*

Then for every odd $g > 1$ there exist a global field K of characteristic p and an ordinary g-dimensional abelian variety X over K that enjoys the following properties:

(i) *All endomorphisms of X are defined over K and $\mathrm{End}^0(X) = E$. In particular, X is absolutely simple.*
(ii) *X is not isogenous over K_a to an abelian variety that is defined over a finite field.*
(ii) *$\mathfrak{g}_{\ell,X} \bigcap \mathbb{Q}_\ell \cdot \mathrm{Id} = \{0\}$, i.e., $\mathfrak{g}_{ell,X}$ does not contain homotheties except zero and $G_{\ell,X} \bigcap \mathbb{Z}_\ell^* \mathrm{Id}$ is finite.*

Remark 1.6. (i) In light of Theorem 2(b) of [17], the second assertion of Theorem 1.5 follows readily from the first one, because in this case

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = \dim_{\mathbb{Q}}(E) = 2 < 2g = 2\dim(X).$$

(ii) In light of Theorem 1.4, the third assertion of Theorem 1.5 follows readily from the first one, because in this case $r(X,E) = g$ is odd.

We prove Theorem 1.5(i) in Section 2. In Section 4 we discuss an explicit example of an abelian variety that satisfies the conditions and conclusions of Theorem 1.4.

I am grateful to B. Poonen, F. Voloch and M. Stoll for a stimulating question that was asked during the special semester "Rational and integral points on higher-dimensional varieties" at the MSRI. My special thanks go to the MSRI and the organizers of this program. I am grateful to the referee, whose comments helped to improve the exposition.

2. Abelian varieties and imaginary quadratic fields

Proof of Theorem 1.5(i). Notice that all endomorphisms of Z are defined over k. (This well-known result goes back to Deuring [3]; it follows easily from Main Theorem of [17].) Since Z is ordinary and $g-1$ is a multiple of $2 = \dim_{\mathbb{Q}}(E)$, a

theorem of Oort -van der Put [7, Th. 1.1] implies the existence of an ordinary g-dimensional abelian variety Y over $k((t))$ with all endomorphisms defined over $k((t))$ and $\mathrm{End}^0(Y)=E$. Clearly, Y and all its endomorphisms are defined over a field K that is finitely generated over k. Now, Mori's specialization arguments [4, Cor. 5.4] allow us to assume that K has transcendence degree 1, i.e., is global. $\square$

3. Ordinary abelian varieties

Lemma 3.1. *Let k be a finite field that consists of q elements, A an ordinary abelian variety over k and d a positive odd integer. If $\{\alpha_1,\dots,\alpha_d\}$ are d eigenvalues of the Frobenius endomorphism Fr of A then $q^{-d}(\prod_{i=1}^d \alpha_i)^2$ is not a root of unity.*

Proof of Lemma 3.1. If $p=\mathrm{char}(k)$ then q is a power of p. Let us choose a p-adic valuation map $\mathrm{ord}_p:\bar{\mathbb{Q}}^*\to\mathbb{Q}$ normalized by the condition $\mathrm{ord}_p(q)=1$. Since A is ordinary, the Honda-Tate theory [16] tells us that $\mathrm{ord}_p(\alpha)=0$ or 1 for every eigenvalue of the Frobenius endomorphism of A. This implies that

$$\mathrm{ord}_p(q^{-d}(\prod_{i=1}^d \alpha_i)^2)=-d+2\sum_{i=1}^d \mathrm{ord}_p(\alpha_i)\in -d+2\mathbb{Z}$$

is an *odd* integer and therefore does not vanish. It follows that $q^{-d}(\prod_{i=1}^d \alpha_i)^2$ is not a root of unity. $\square$

Proof of Theorem 1.4. Replacing (if necessary) K by its finite separable algebraic extension, we may and will assume that all endomorphisms of X are defined over K; in particular, $E\subset \mathrm{End}^0_K(X)=\mathrm{End}^0(X)$. Let us assume that $\mathfrak{g}_{\ell,X}\bigcap \mathbb{Q}_\ell\cdot\mathrm{Id}\ne\{0\}$. This means that $\mathfrak{g}_{\ell,X}$ contains $\mathbb{Q}_\ell\cdot\mathrm{Id}$ and therefore $\mathfrak{c}=\mathbb{Q}_\ell\cdot\mathrm{Id}$.

Let us put $G^0=G_{\ell,X}\bigcap SL(V_\ell(X))$. Clearly, G^0 is a closed (compact) Lie subgroup of $G_{\ell,X}$ and $\mathrm{Lie}(G^0)$ has codimension 1 in $\mathrm{Lie}(G_{\ell,X})=\mathfrak{g}^{ss}\oplus\mathbb{Q}_\ell\cdot\mathrm{Id}$. The semisimplicity of $\mathfrak{g}^{ss}$ implies that $\mathrm{Lie}(G^0)=\mathfrak{g}^{ss}$.

Let us put

$$S=G_{\ell,X}\bigcap(1+\ell^2\mathbb{Z}_\ell)\mathrm{Id}\subset\mathbb{Z}_\ell^*\mathrm{Id}.$$

Clearly, S is compact. Since $\mathfrak{g}_{\ell,X}=\mathrm{Lie}(G_{\ell,X})$ contains $\mathbb{Q}_\ell\cdot\mathrm{Id}$, the group $G_{\ell,X}$ contains an open subgroup of $\mathbb{Z}_\ell^*\mathrm{Id}$. It follows that S is an open subgroup of finite index in $\mathbb{Z}_\ell^*\mathrm{Id}$. Since $1+\ell^2\mathbb{Z}_\ell$ does not contain nontrivial roots of unity, S does not contain elements of finite order (except Id) and therefore $G^0\bigcap S=\{\mathrm{Id}\}$. Recall that both G^0 and S are subgroups of $G_{\ell,X}$. Let us consider the homomorphism of compact ℓ-adic Lie groups

$$\pi: G^0\times S\to G_{\ell,X},\ (u,c)\mapsto uc=cu.$$

Clearly, π is injective and the corresponding tangent map of Lie algebras is an isomorphism. It follows that $G^1:=\pi(G^0\times S)$ is an open compact subgroup in $G_{\ell,X}$ and π induces an isomorphism of ℓ-adic Lie groups $G^0\times S$ and G^1.

Lemma 3.2. *There exists a positive integer m such that*

$$\det_{E_\ell}(g)^m\in\mathbb{Q}_\ell^*\mathrm{Id}\ \forall g\in G_{\ell,X}.$$

Proof of Lemma 3.2. Since $\mathrm{Lie}(G^0)$ is semisimple, it follows from Remark 1.2 that $\det_{E_\ell}(G^0)$ is a finite group. If m_0 is its order then $\det_{E_\ell}(g_0)^{m_0}=1$ for all $g_0\in G^0$. Notice that

$$\det_{E_\ell}(c)=c^{r(X,E)}\ \forall c\in\mathbb{Z}_\ell^*\mathrm{Id},$$

because $\mathbb{Z}_\ell^*\mathrm{Id} \subset E_\ell^*$. It follows that $\det_{E_\ell}(g)^{m_0} \in \mathbb{Q}_\ell^*\mathrm{Id}\ \forall g \in G^1$. In order to finish the proof, one has only to recall that G^1 is a subgroup of finite index in $G_{\ell,X}$ and put $m := m_0 \cdot [G_{\ell,X} : G^1]$. □

There exists a place v of K such that the abelian variety X has ordinary good reduction. (In fact, this condition is fulfilled for all but finitely many places of K.) Let $k(v)$ be the residue field at v, let $q(v)$ be the cardinality of $k(v)$ and $X(v)$ the reduction of X at v, which is an ordinary abelian variety over $k(v)$ whose dimension coincides with $\dim(X)$. Let $\mathbb{P}_v(t) \in \mathbb{Z}[t]$ be the (degree $2\dim(X)$) characteristic polynomial of the Frobenius endomorphism Fr of $X(v)$. One may view the roots of $\mathbb{P}_v$ as eigenvalues of the Frobenius endomorphism with respect to its natural action on $V_\ell(X(v))$.

Let us choose a place $\bar{v}$ of K_a that lies above v. Such a choice gives rise to natural isomorphisms [12, 10]

$$T_\ell(X) \cong T_\ell(X(v)),\ V_\ell(X) \cong V_\ell(X(v))$$

in such a way that $\mathrm{Fr} \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X(v))$ corresponds to a certain element of $G_{\ell,X}$: this element is called the *Frobenius element* attached to $\bar{v}$ and denoted by $F_{\bar{v}}$. It is known [14, Chap. 7, proof of Prop. 7.23] (see also [19, p. 167]) that

$$b_v := \det_{E_\ell}(F_{\bar{v}}) \in E^* \subset E_\ell^*$$

and b_v is a product of $r(X,E)$ eigenvalues of Fr.

In other words, let L be the splitting field of $\mathbb{P}_v(t)$ over E: it is a finite Galois extension of E. Then there exist roots $\alpha_1, \dots, \alpha_{r(X,E)}$ of $\mathbb{P}_v(t)$ such that their product coincides with b_v. On the other hand, it follows from a famous theorem of A. Weil (the Riemann hypothesis) [5, Sect. 21] that if we fix a field embedding $L \subset \mathbb{C}$ then

$$\mid b_v^2 \mid_\infty = q(v)^{r(X,E)}$$

where $\mid\ \mid_\infty$ is the standard (archimedean) absolute value on the field of complex numbers. On the other hand, by Lemma 3.2, there exists a positive integer m such that $b_v^m \in \mathbb{Q}_\ell$. Since the intersection of $E = E\otimes 1$ and $\mathbb{Q}_\ell = 1\otimes\mathbb{Q}_\ell$ in $E_\ell = E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ coincides with $\mathbb{Q}$, we conclude that b_v^m is a rational number. This implies that b_v^{2m} is a positive rational number and, by Weil's theorem, coincides with $q(v)^{mr(X,E)}$. This implies that

$$1 = \left(q(v)^{-r(X,E)} \cdot b_v^2\right)^m.$$

However, by Lemma 3.1, $q(v)^{-r(X,E)}b_v^2$ is *not* a root of unity. (Here we use the *oddity* of $r(X,E)$.) We get a contradiction, which proves the Theorem. □

4. Superelliptic jacobians

Proposition 4.1. *Let K be a number field with the ring of integers $\mathcal{O}_K$. Let Y be an abelian variety of positive dimension over K, let L be a CM-field of degree $2\dim(X)$ and $i : L \hookrightarrow \mathrm{End}^0(Y)$ an embedding that sends 1 to 1_Y. Let p be a prime that splits completely in L, i.e. $L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ splits into a product of $[L : \mathbb{Q}]$ copies of $\mathbb{Q}_p$. Let $\mathfrak{p}$ be maximal ideal in $\mathcal{O}_K$ with residual characteristic p.*

If Y has good reduction at $\mathfrak{p}$ then this reduction is ordinary.

Proof. Let $\bar{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$. Let $L_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of L. By assumption, $L_{\mathfrak{p}} = \mathbb{Q}_p$ and therefore the set $H_{\mathfrak{p}}$ of $\mathbb{Q}_p$-linear field embeddings

$L_{\mathfrak{p}} \hookrightarrow \bar{\mathbb{Q}}_p$ is a singleton that consists of the inclusion map $\mathbb{Q}_p \subset \bar{\mathbb{Q}}_p$; in particular, $\#(H_{\mathfrak{p}}) = 1$. Now the assertion follows readily from Lemma 5 in Sect. 4 of [16]. □

Lemma 4.2. *Let us consider the curve $C_0 : y^3 = x^9 - x$ and its jacobian $J(C_0)$ over $\mathbb{Q}$.*

Then:

(i) *If p is a prime such that $p-1$ is divisible by 24 then $J(C_0)$ has ordinary good reduction at p.*

(ii) *$J(C_0)$ is a (non-simple) abelian variety of CM-type over $\bar{\mathbb{Q}}$.*

Proof. Clearly, both C_0 and $J(C_0)$ have good reduction at p, because $x^9 - x = x(x^8-1)$ has 9 distinct roots in $\mathbb{F}_p$ and therefore has no multiple roots in characteristic p. In order to check that $J(C_0)$ has ordinary reduction, pick a number field F such that F contains $\mathbb{Q}(\zeta_{24})$, all endomorphisms of $J(C_0)$ are defined over F and all homomorphisms between $J(C_0)$ and the elliptic curve $y^2 = x^3 - x$ are defined over F. Let us consider both C_0 and $J(C_0)$ over F, and let $\mathfrak{p}$ be a place of F that lies above p. For our purposes, it suffices to check that $J(C_0)$ has ordinary reduction at $\mathfrak{p}$.

Pick a primitive cubic root of unity $\zeta_3 \in F$. Then the map

$$(x, y) \mapsto (x, \zeta_3 y)$$

induces an automorphism $\delta_3 : C_0 \to C_0$, which, in turn, induces by Albanese functoriality an automorphism $J(C_0) \to J(C_0)$, which we still denote by δ_3. It is known [8, p. 149] that $\delta_3^2 + \delta_3 + 1 = 0$ in $\mathrm{End}(J(C_0))$, which leads to the embedding

$$\mathbb{Z}[\zeta_3] \hookrightarrow \mathrm{End}(J(C_0)),\ \zeta_3 \mapsto \delta_3, 1 \mapsto 1_{J(C_0)}.$$

Extending it by $\mathbb{Q}$-linearity, we get an embedding

$$\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \hookrightarrow \mathrm{End}^0(J(C_0)),\ \zeta_3 \mapsto \delta_3, 1 \mapsto 1_{J(C_0)}.$$

On the other hand, pick a primitive 8th root of unity $\zeta_8 \in F$. Then the map

$$(x, y) \mapsto (\zeta_8^{-1} x, \zeta_8^{-3} y)$$

induces an automorphism $\delta_8 : C_0 \to C_0$, which commutes with δ_3. Again δ_8 induces by Albanese functoriality an automorphism of $J(C_0)$, which we still denote by δ_8; clearly δ_8 and δ_3 do commute in $\mathrm{End}(J(C_0)$. In order to understand δ_8 better, let us divide both sides of the equation for C_0 by $x^9 = (x^3)^3$: we get $(y/x^3)^3 = 1 - (1/x)^8$. It follows that C is F-birationally isomorphic to the curve

$$C' : w^8 = -u^3 + 1;\ w = 1/x, u = y/x^3$$

and δ_8 is induced by

$$(u, w) \mapsto (u, \zeta_8 w).$$

This implies that the jacobian $J(C')$ of C' and $J(C)$ are isomorphic over F. Let us put $f(w) = -w^3 + 1$. Then in notations of [21], $C' = C_{f,8}$ and the structure of its jacobian $J(C') = J(C_{f,8})$ is described as follows [21, Sect. 5, Cor. 5.12, Rem. 5.14, Th. 5.17]. First, $J(C_{f,8})$ contains a δ_8-invariant abelian fourfold

$$J^{(f,8)} = (\delta_8^3 + \delta_8^2 + \delta_8 + 1)(J(C_{f,8})) \subset J(C_{f,8})$$

provided with an embedding

$$\mathbb{Z}[\zeta_8] \hookrightarrow \mathrm{End}(J^{(f,8)}),\ \zeta_8 \mapsto \delta_8, 1 \mapsto 1_{J(C_{f,8})}.$$

Clearly, $J^{(f,8)}$ is δ_3-invariant. This gives rise to an embedding

$$\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\zeta_3) \otimes \mathbb{Q}(\zeta_8) \hookrightarrow \mathrm{End}^0(J^{(f,8)}),\ \zeta_3 \mapsto \delta_3, \zeta_8 \mapsto \delta_8$$

and 1 goes to the identity map. This implies that $J^{(f,8)}$ is an abelian fourfold of CM-type. Since p splits in $\mathbb{Q}(\zeta_{24})$, it follows from Proposition 4.1 that $J^{(f,8)}$ has ordinary reduction at all places of F over p. Second, $J(C_{f,8})$ is isogenous (over F) to a product of $J^{(f,8)}$, two copies of the elliptic curve $y^2 = x^3 - x$ and the elliptic curve $w^2 = -v^3 + 1$. Since 24 divides $p - 1$, the prime p splits in the imaginary quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Therefore the CM-elliptic curves $y^2 = x^3 - x$ with multiplication by $\mathbb{Q}(\sqrt{-1})$ and $w^2 = -v^3 + 1$ with multiplication by $\mathbb{Q}(\sqrt{-3})$ have ordinary reduction at p. It follows that $J(C_{f,8})$ has ordinary reduction at $\mathfrak{p}$. $\square$

Example 4.3. Fix a prime p with $p - 1$ divisible by 24, let $K = \mathbb{F}_p(t)$ and let X be the 7-dimensional jacobian of the K-curve $C : y^3 = x^9 - x - t$. Since p divides neither 9 nor 8, $x^9 - x \in \mathbb{F}_p[x]$ is a *Morse polynomial* [11, p. 39], i.e., its derivative $9x^8 - 1$ has 8 distinct roots $\beta_1, \dots, \beta_8$ and all eight critical values $\beta_i^9 - \beta_i = -\frac{8}{9}\beta_i$ are distinct. It follows that the Galois group of $x^9 - x - t$ over $\mathbb{F}_p(t)$ is the full symmetric group $\mathbf{S}_9$ [11, p. 41]. On the other hand, if $\zeta \in \mathbb{F}_p$ is a primitive cubic root of unity then

$$(x, y) \mapsto (x, \zeta y)$$

gives rise to a non-trivial automorphism of C (of period 3), which, in turn, allows us to define the embedding

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \hookrightarrow \mathrm{End}^0(J(C)),\ 1 \mapsto 1_{J(C)}.$$

By Theorem 0.1 of [20], $E = \mathbb{Q}(\sqrt{-3})$ coincides with its own centralizer in $\mathrm{End}^0(J(C))$ and therefore contains $\mathfrak{C}(J(C))$. This means that $\mathfrak{C}(J(C)) = E$ or $\mathbb{Q}$. On the other hand, the reduction of $J(C)$ at $t = 0$ is the jacobian of the $\mathbb{F}_p$-curve $y^3 = x^9 - x$, which is ordinary, by Lemma 4.2. Applying Theorem 1.4, we obtain that $\mathfrak{g}_{\ell,J(C)}$ does not contain non-zero homotheties. On the other hand, if $\mathfrak{C}(J(C)) = \mathbb{Q}$ then, by Theorem 1.3(III), $\mathfrak{g}_{\ell,J(C)}$ does contain all the homotheties. This contradiction proves that $\mathfrak{C}(J(C)) = E$ and therefore the centralizer of E coincides with the whole $\mathrm{End}^0(J(C))$. This implies that $\mathrm{End}^0(J(C)) = E$ and therefore $J(C)$ is absolutely simple and is not of CM-type. It follows that $J(C)$ is not isogenous to an abelian variety that is defined over a finite field.

References

[1] F. A. Bogomolov, *Sur l'algébricité des représentations ℓ-adiques.* C.R. Acad. Sci. Paris Sér. A-B (1980), no. 15, A701–A703.

[2] F. A. Bogomolov, *Points of finite order on an abelian variety.* Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), 782–804; Math. USSR Izv. **17** (1981), 55–72.

[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hamburg **14** (1941), 197–272.

[4] Sh. Mori, *On Tate conjecture concerning endomorphisms of abelian varieties.* Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), pp. 219–230, Kinokuniya Book Store, Tokyo, 1978.

[5] D. Mumford, Abelian varieties, 2nd edn, Oxford University Press, 1974.

[6] F. Oort, *The isogeny class of a CM-abelian variety is defined over a finite extension of the prime field.* J. Pure Applied Algebra **3** (1973), 399–408.

[7] F. Oort, M.-van der Put, *A construction of an abelian variety with a given endomorphism algebra.* Compositio Math. **67** (1988), 103–120.

[8] B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141–188.
[9] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications.* Amer. J. Math. **98** (1976), 751–804.
[10] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, 2nd edition, Addison Wesley, 1989.
[11] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, Boston-London, 1992.
[12] J-P. Serre, J. Tate, *Good reduction of abelian varieties.* Ann. of Math. (2) **88** (1968), 492–517.
[13] J.-P. Serre, Lie algebras and Lie groups, 2nd edition, Springer Lecture Notes in Math. **1500** (1992).
[14] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan **11**, Princeton University Press, 1971.
[15] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, Princeton, 1997.
[16] J. Tate, *Classes d'isogénie des variétes abéliennes sur un corps fini (d'aprés Honda).* Séminaire Bourbaki **352** (1968). Springer Lecture Notes in Math. **179** (1971), 95–110.
[17] J. Tate, *Endomorphisms of abelian varieties over finite fields.* Inv. Math. **2** (1966), 134–144.
[18] Yu. G. Zarhin, *Torsion of abelian varieties in finite characteristic*. Mat. Zametki **22** (1977), 3–11; Math. Notes **22** (1978), 493–498.
[19] Yu. G. Zarhin, *Abelian varieties, ℓ-adic representations and Lie algebras. Rank independence on ℓ*. Inv. Math. **55** (1979), 165 - 176.
[20] Yu. G. Zarhin, Endomorphism rings of certain jacobians in finite characteristic. Matem. Sbornik **193** (2002), issue 8, 39–48; Sbornik Math., 2002, **193** (8), 1139-1149.
[21] Yu. G. Zarhin, *Superelliptic jacobians*. arXiv:math.AG/0601072; to appear in Proceedings of the Pisa research programme on Diophantine Geometry (Spring 2005).

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia
E-mail address: `zarhin@math.psu.edu`